IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEARCH OF 4204 NORTH HENDERSON ROAD #1, ARLINGTON, VIRGINIA 22203	**UNDER SEAL** 1:22-SW-124

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH AND SEIZURE WARRANT

I, Randall M. Mason, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 4204 North Henderson Road #1, Arlington, Virginia 22203 ("**TARGET LOCATION**") further described in Attachment A, for the things described in Attachment B.

2. As explained herein, there is probable cause to believe that criminal violations of 21 U.S.C. §§ 841(a)(1) and 846 (conspiracy to distribute cocaine base and distribution of cocaine base) have been committed by MARLOW DEMONTE TERRY at the **TARGET LOCATION**. There is also probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as further described in Attachment B, will be found at the **TARGET LOCATION**.

3. I am a Detective with the Arlington County Police Department. I have been employed as a police officer with the Arlington County Police Department since 2007. I have been assigned to the Vice/Narcotics Unit since 2014. I am currently assigned to the Drug Enforcement Administration ("DEA"), where I am federally deputized as a Task Force Officer ("TFO") with the DEA's High Intensity Drug Trafficking Area Task Force. As such, I am a Law Enforcement Officer as defined under Section 2510(7) of Title 18, United States Code, (*i.e.* an

officer of the United States or a political sub-division thereof, who is empowered to conduct investigations of, and to make arrests for, offenses enumerated in Title 21, United States Code.) During my time in law enforcement, I have participated in the application for and execution of numerous arrest and search warrants in the investigation of narcotics and organized crime related offenses, resulting in the prosecution and conviction of numerous individuals and the seizure of illegal drugs, weapons, stolen property, and other evidence of criminal activity.

4. During my time in law enforcement, I have investigated violations of federal and state narcotics laws. I have conducted or participated in numerous investigations involving narcotics-related offenses, which have resulted in the seizure of illegal drugs, drug proceeds in the form of United States currency, weapons, and other evidence of criminal activity. My experience includes the execution of search warrants. These investigations have led to the arrest and conviction of drug distributors and users in the General District, Juvenile and Domestic Relations, and Circuit Courts of Arlington County, as well as in the Eastern District of Virginia. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology used by drug traffickers and abusers of controlled dangerous substances. Through my employment, I have gained knowledge in the use of various investigative techniques including the use of wiretaps, physical surveillance, undercover agents, confidential informants and cooperating witnesses, the controlled purchase of illegal narcotics, electronic surveillance, consensually monitored recordings, investigative interviews, financial investigations, the service of administrative and grand jury subpoenas, and the execution of search and arrest warrants. I have testified at trials, in grand jury proceedings, and at preliminary hearings, and I have been certified as an expert in the distribution of narcotics in Arlington County General District and Circuit Courts.

5. The facts and information contained in this affidavit are based upon my personal knowledge of the investigation and observations of other law enforcement officers and agents involved in this investigation. All observations referenced below that were not personally made by me were related to me by the persons who made such observations. Additionally, unless otherwise noted, wherever your Affiant asserts that a statement was made by an individual, such statement is described in substance herein, and is not intended to be a verbatim recitation of such statement.

6. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

7. The United States, including the Drug Enforcement Administration, is conducting a criminal investigation of MARLOW DEMONTE TERRY and others regarding possible violations of 21 U.S.C. §§ 841(a)(1) and 846 (conspiracy to distribute and distribution of cocaine base).

8. The investigation began in or around March 2021 when the Arlington County Police Department's Organized Crime Section, Narcotics Enforcement Unit received information from CS-1 identifying coconspirator WILLIAM MAURICE JOHNSON (a.k.a. "We Will") as a distributor of cocaine base in Arlington County and elsewhere. Additional sources of information were developed and provided historical information regarding TERRY and JOHNSON's cocaine base distribution.

A. Sources of information.

9. ***Cooperating Source-1.*** CS-1 became a confidential source with the Arlington County Police Department in or about March 2021. CS-1 is a paid informant and does not have

any pending criminal charges in Arlington County. On February 22, 2022, CS-1 was summoned to appear in Alexandria District Court for two misdemeanor charges of phone threats and taking nude photographs without consent. CS-1 is an admitted drug user and distributor and has prior convictions for assault and battery, theft, domestic assault and battery, credit card fraud, violation of a protection order, ID theft, robbery, burglary, theft, receiving stolen property, possession of a controlled substance, credit card theft, embezzlement, possession with intent to distribute schedule I/II drugs, and probation violations. The information that CS-1 has provided to law enforcement has been proven true and accurate. With respect to the instant case, CS-1's information has been corroborated by other confidential sources, information obtained from various public databases, physical surveillance, cell phone data extractions, and other information obtained during the investigation. To my knowledge, none of the information provided by CS-1 has proved to be false, misleading, or inaccurate in any material respect. CS-1 has made statements against his own penal interest. For these reasons, I consider CS-1 to be reliable.

10. ***Cooperating Source-2.*** CS-2 became a confidential source with the Arlington County Police Department in or about November 2018. CS-2 has a pending criminal charge in California, dating to 1999, for an offense involving dangerous drugs under California law. The offense is not extraditable. CS-2 is a paid informant. CS-2 is an admitted drug user and has prior convictions for theft, escape, trespassing, disorderly conduct, assault and battery, petit larceny, distribution of a controlled dangerous substance, possession of controlled dangerous substance with intent to distribute, obtaining money by false pretenses, and probation violation. The information that CS-2 has provided to law enforcement has been proven true and accurate. With respect to the instant case, CS-2's information has been corroborated by other confidential

sources, information obtained from various public databases, physical surveillance, cell phone data extractions, and other information obtained during the investigation. To my knowledge, none of the information provided by CS-2 has proved to be false, misleading, or inaccurate in any material respect. CS-2 has made statements against his own penal interest. For these reasons, I consider CS-2 to be reliable.

11. ***Cooperating Source-3***. CS-3 became a source of information with the Arlington County Police Department in or about March 2021 following his arrest for larceny and robbery by force. CS-3 is an admitted drug user and has prior convictions for a false statement to an officer, destruction of property, theft, shoplifting, housebreaking, concealment of merchandise, grand larceny, and probation violation. The information that CS-3 has provided to law enforcement has been proven true and accurate. With respect to the instant case, CS-3's information has been corroborated by other confidential sources, information obtained from various public databases, physical surveillance, cell phone data extractions, and other information obtained during the investigation. To my knowledge, none of the information provided by CS-3 has proved to be false, misleading, or inaccurate in any material respect. CS-3 has made statements against his own penal interest. For these reasons, I consider CS-3 to be reliable.

12. ***Cooperating Source-4***. CS-4 became a confidential source with the Arlington County Police Department in or about September 2012. CS-4 does not have any pending criminal charges and is a paid informant. CS-4 is an admitted drug user and has prior convictions for possession of drug paraphernalia, larceny, failure to appear, trespassing, possession of controlled substances, unlawful wounding, and probation violation. The information that CS-4 has provided to law enforcement has been proven true and accurate. With respect to the instant

case, CS-4's information has been corroborated by other confidential sources, information obtained from various public databases, physical surveillance, cell phone data extractions, and other information obtained during the investigation. To my knowledge, none of the information provided by CS-4 has proved to be false, misleading, or inaccurate in any material respect. CS-4 has made statements against his own penal interest. For these reasons, I consider CS-4 to be reliable.

B. Evidence of the conspiracy and cocaine base distribution.

13. ***Historical Information provided by CS-1.*** In April 2021, CS-1 stated that he had been JOHNSON's customer for approximately seven months, buying approximately six grams of cocaine base a week during that timeframe. CS-1 said that he had purchased cocaine base from JOHNSON inside of TERRY's residence on several occasions when JOHNSON was alone inside of TERRY's residence. Additionally, CS-1 has observed JOHNSON "cooking" cocaine base at TERRY's apartment, which is located in Arlington, Virginia. Through these interactions, as well as other conversations with JOHNSON, CS-1 stated that he knew that JOHNSON was supplying TERRY with cocaine base for further distribution.

14. ***Historical Information provided by CS-2.*** In June 2021, CS-2 met with detectives and stated that he had been purchasing cocaine base from TERRY for approximately the past year. CS-2 stated that he had purchased $100 worth of cocaine base, approximately one gram, around 100 times in the last year. CS-2 positively identified a photograph of TERRY and provided TERRY's phone number and residence. CS-2 stated that he observed TERRY with up to approximately four ounces of suspected cocaine in TERRY's residence, which TERRY later "cooked" into cocaine base.

15. ***Historical Information provided by CS-3.*** In or about March 2021, CS-3 was arrested by the Arlington County police in relation to a larceny and robbery by force. During the interview with the robbery detective, CS-3 provided information about cocaine base sales in Arlington County. Arlington County Narcotics Detective Ouzidane conducted an interview on this topic with CS-3, who told Detective Ouzidane that CS-3 regularly purchased cocaine base from TERRY. CS-3 provided TERRY's approximate residence location, which matched information known to detectives. CS-3 stated that he was inside of TERRY apartment on or about March 22, 2021 and purchased $50 of cocaine base from TERRY. CS-3 stated that TERRY had a large surplus of cocaine base at time and described it as a large cookie.

16. Two additional interviews were completed with CS-3. CS-3 stated during those interviews that he had purchased from TERRY for approximately the past two years. On average, CS-3 stated that he purchased cocaine base from TERRY approximately 10 times per week during that timeframe. CS-3 stated that the smallest amount he ever purchased from TERRY was $50 worth, approximately 0.5 grams, because TERRY wouldn't sell smaller amounts. The largest amount of cocaine base that CS-3 ever purchased from TERRY at one time was $200 worth, approximately two grams. The largest amount of cocaine base that CS-3 has ever seen TERRY with was approximately the size of a baseball.

17. ***Historical Information provided by CS-4.*** CS-4 has been an informant with Arlington County Police Department since 2012 and does not have any pending criminal charges. In May 2021, detectives met with CS-4 to see if CS-4 had any information about the instant case. CS-4 identified a photograph of TERRY and stated that he had been purchasing approximately $200 worth of cocaine base, or approximately two grams, once a month for the past year. In total, CS-4 stated that he purchased approximately 24 grams of cocaine base from

TERRY in the last year. CS-4 stated he had been present when TERRY was cooking cocaine base inside of TERRY's residence in both the microwave and on the stove top.

18. ***Additional investigative techniques.*** During this investigation, law enforcement has gatherer historical information regarding the DTO from approximately 11 different confidential sources. Tolls for the co-conspirators were subpoenaed and examined to identify other potential customers and co-conspirators. Law enforcement has conducted physical surveillance and observed suspected drug transactions. Law enforcement also subpoenaed CashApp and examined the returns, identifying suspected money transactions related to narcotics deals.

19. ***February 4, 2022 controlled purchase.*** On or about February 4, 2022, under the direction and control of law enforcement, CS-4 contacted TERRY to arrange to purchase $100 worth of cocaine base. Law enforcement observed TERRY exit the **TARGET LOCATION** building and meet with two unknown individuals.

20. TERRY then got into a vehicle as the driver with two unknown individuals as passengers. CS-4 directed TERRY to a predetermined meeting location in Arlington, Virginia. TERRY advised CS-4 that he needed to drop off his unknown passengers before meeting. Law enforcement searched CS-4 prior to CS-4 going to the meeting. No contraband or United States currency was location. CS-4 was given $100 in pre-recorded evidence funds for the purchase. CS-4 was under constant law enforcement surveillance. Upon arriving, law enforcement observed CS-4 meet with TERRY. CS-4 provided TERRY with the $100 in pre-recorded evidence funds. CS-4 received a quantity of cocaine base from TERRY. CS-4 returned to a predetermined meet location where he gave law enforcement the cocaine base. CS-4 was

searched a second time for contraband or United States currency and none was located. A field test was conducted on the suspected cocaine base and a positive response was obtained.

21. TERRY was observed entering back into the **TARGET LOCATION** building approximately 10 minutes after CS-4 exited TERRY's vehicle.

22. ***February 18, 2022 controlled purchase.*** On or about February 18, 2022, under the direction and control of law enforcement, CS-4 contacted TERRY to arrange to purchase $200 worth of cocaine base. CS-4 directed TERRY to a predetermined meeting location in Arlington, Virginia. Approximately 7 minutes after CS-4 and TERRY hung up the phone, TERRY was observed exiting the **TARGET LOCATION** building. Law enforcement searched CS-4 prior to CS-4 going to the meeting. No contraband or United States currency was located. CS-4 was given $200 in pre-recorded evidence funds for the purchase. CS-4 was under constant law enforcement surveillance. Upon arriving, law enforcement observed CS-4 meet with TERRY. CS-4 provided TERRY with the $200 in pre-recorded evidence funds. CS-4 received a quantity of cocaine base from TERRY. CS-4 returned to a predetermined meet location where he gave law enforcement the cocaine base. CS-4 was searched a second time for contraband or United States currency and none was located. A field test was conducted on the suspected cocaine base and a positive response was obtained.

23. TERRY was observed entering back into the **TARGET LOCATION** building approximately 10 minutes after CS-4 exited TERRY's vehicle.

TARGET LOCATION

24. Your Affiant searched TERRY in a number of law enforcement databases. None of the databases showed a current address other than the **TARGET LOCATION.** TERRY's last interaction with law enforcement was in October 2021 in Fairfax, Virginia. During that

interaction with the Fairfax Police Department, TERRY gave the **TARGET LOCATION** as his address. TERRY has a current license in Virginia that was issued in December 2021 and the listed address is the **TARGET LOCATION**.

25. Throughout this investigation, law enforcement has obtained three different phone numbers utilized by TERRY. Through administrative subpoenas, Your Affiant learned two phone numbers were serviced by T-Mobile and listed TERRY as the subscriber and the **TARGET LOCATION** as the subscriber address. Through a separate administrative subpoena, Your Affiant learned that AT&T currently services TERRY's most recent phone number and that TERRY is the listed subscriber; the **TARGET LOCATION** is listed as the subscriber address. Further, this phone number was used to coordinate the two most recent controlled purchases occurring on February 4, 2022 and February 18, 2022.

26. On or about February 22, 2022, Your Affiant served an administrative subpoena on AHC, the property management company for the **TARGET LOCATION.** The information returned to Your Affiant from AHC showed that TERRY was on the lease for the **TARGET LOCATION** and was the only individual on the lease.

27. The Arlington County Police Department placed a pole camera outside of the **TARGET LOCATION** that viewed the front door to the building. Since the installation of the camera, law enforcement has observed TERRY going in and out of the **TARGET LOCATION** building on a regular basis.

28. On February 22, 2022, Your Affiant conducted physical surveillance and observed TERRY enter and exit the building for the **TARGET LOCATION** using a key for entry.

USE OF CELLULAR TELEPHONES/STORAGE MEDIA BY DRUG TRAFFICKERS

29. Based on my training, experience, and participation in narcotics and drug-related investigations, and my knowledge of this case, I am aware that:

a. Drug traffickers commonly utilize cellular phones, as well as other communication devices, to keep in constant contact with their suppliers, associates, and clients in drug trafficking.

b. Drug traffickers commonly utilize and possess multiple cellular phones at any given time. It is common for drug traffickers to use one cell phone as a personal number that they attempt to limit the numbers of contacts with other co-conspirators involved in their trade. Drug traffickers commonly utilize a second phone as their "work" phone that is used in their business. This second phone utilized for business purposes is often not in the drug trafficker's name. The second phone is also commonly changed, either by changing phones entirely or changing the phone number of the second phone. All of these things are done by drug traffickers in an attempt to avoid detection by law enforcement.

c. Drug traffickers commonly make and maintain business records. Specifically, it is quite common for those involved in the manufacture, sale, purchase, and transportation of controlled substances to generate and maintain writings, books, records, receipts, notes, ledgers, lists, airline tickets, money orders, package and shipping labels, and other memoranda to assist in their criminal activities. These materials are created and maintained in much the same way and for the same reasons as persons involved in legitimate businesses. Drug traffickers maintain records in order to know the current status of the various illegal transactions in which they are involved. Without the aid of such records, drug traffickers would face a high

possibility of error and mistake due to the number, complexity, and frequency of their transactions, and the clandestine nature of drug trafficking activities. These business records are often located within the contents of the drug trafficker's cell phone(s).

d. Drug traffickers commonly maintain addresses or telephone numbers in books or papers, which reflect names, addresses and/or telephone numbers of their associates in drug trafficking. They also store such information, as well as photographs, messages, and personal notes, in electronic equipment including, but not limited to, cellular phones.

e. Drug traffickers commonly keep their old cell phones. It is common for law enforcement to seize numerous old cell phones during the execution of a search warrant at a drug trafficker's residence.

30. I know from my training and experience, as well as from information found in publicly available materials, including those published by cellular phone providers, that some makes and models of cellular phones offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") and facial scan in lieu of a numeric or alphanumeric passcode or password. These features are called Touch ID and Face ID.

31. If a user enables Touch ID or Face ID on a given cellular phone device, he or she can register fingerprints or a facial scan that can be used to unlock that device. The user can then use any of the registered fingerprints or facial scans to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor or showing his or her face to the cellphone camera. In my training and experience, users of cellular phone devices that offer Touch ID or Face ID often enable those features because they are considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more

secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

32. In some circumstances, a fingerprint or facial scan cannot be used to unlock a device that has Touch ID or Face ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID or Face ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked cellular phone device, the opportunity to unlock the device via Touch ID or Face ID exists only for a short time. Touch ID or Face ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made.

33. The passcode or password that would unlock the cellular phone is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of the cellular phone to the device's Touch ID sensor or use the device's Face ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant cellular phone device(s) via Touch ID with the use of the fingerprints of the user(s) or Face ID with the use of the face of the user is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

34. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the

device. However, in my training and experience, that person may not be the *only* user of the device whose fingerprints are among those that will unlock the device via Touch ID or Face ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Further, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the **TARGET LOCATION** to press their finger(s) against the Touch ID sensor or show their face to the Face ID sensor of any locked cellular phone device(s) found during the search of the **TARGET LOCATION** in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID or Face ID.

35. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled cellular phone device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the cellular phone as described above within the attempts permitted by Touch ID or Face ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

36. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the **TARGET LOCATION** to the Touch ID sensor of cellular phones for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant. I also request that the Court authorize law enforcement to show the face of individuals found at the **TARGET LOCATION** to the

Face ID sensor of cellular phones for the purpose of attempting to unlock the device via Face ID in order to search the contents as authorized by this warrant.

TECHNICAL TERMS

37. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include cellular telephones, hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

38. As described above and in Attachment B, this application seeks permission to search for records that might be found at the property described in Attachment A, in whatever

form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, including a cellular phone. Thus, the warrant would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

39. *Probable cause*. I submit that if a computer or storage medium, including a cellular telephone, is found at the property described in Attachment A, there is probable cause to believe that it will include evidence, contraband, fruits, and/or instrumentalities of criminal activities for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files or remnants of deleted files may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples,

this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

40. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate and search not only computer files that might serve as direct evidence of the crimes described on the warrant, but also seeks permission to locate and search forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the property described in Attachment A because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates

files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored

within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is

evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

41. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to

obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data at the property described in Attachment A. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

42. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I am applying would permit seizing, imaging, or otherwise copying storage media that reasonably appears to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

43. Based on the information provided in this affidavit, your Affiant submits that probable cause exists to believe that evidence of narcotics trafficking in violation of 21 U.S.C. §§ 841(a)(1) and 846, specifically those items set forth in Attachment B, are contained within the **TARGET LOCATION**, further described in Attachment A. Accordingly, your Affiant respectfully requests a warrant to search the **TARGET LOCATION**.

Respectfully submitted,

Task Force Officer Randall Mason
Drug Enforcement Administration

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on February 28, 2022.

John F. Anderson Digitally signed by John F. Anderson
Date: 2022.02.28 16:03:10 -05'00'

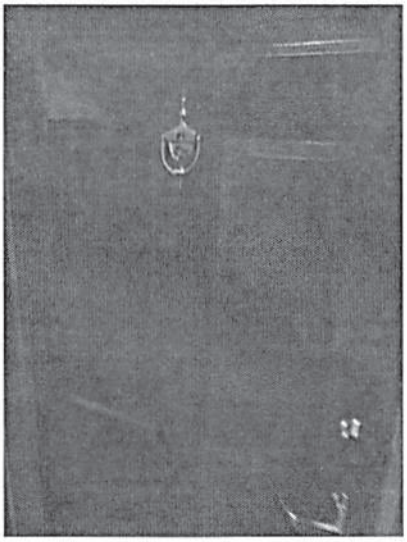
Hon. John F. Anderson
United States Magistrate Judge

ATTACHMENT A

Place to be searched

The address known as 4204 North Henderson Road #1, Arlington, Virginia 22203 (**"TARGET LOCATION"**) is an apartment within a garden style apartment building. The building is two stories and is constructed of red brick. The door to the apartment building is dark red in color with "4204" affixed below a window. After entering the building, apartment #1 is to the left. The door to the apartment is red in color with silver fixtures. The silver door knocker in the middle of the door has "#1" engraved on it.

Exterior door



Door to apartment #1

ATTACHMENT B

Items to be seized

All items constituting evidence and/or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) and 846 (conspiracy to distribute cocaine base and distribution of cocaine base) including, but not limited to, the following:

a. Controlled substances, packaging materials, indicia of distribution, records and documents, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the ordering, purchase or possession of controlled substances;

b. U.S. currency and other illicit gains from the distribution of controlled substances;

c. Books, records, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the ordering, purchase or possession of controlled substances;

d. Address and/or telephone books and papers, including computerized or electronic addresses and/or telephone records reflecting names, addresses and/or telephone numbers;

e. Books, records, receipts, bank statements, and records, money drafts, letters of credit, money order and cashier's checks, receipts, pass books, bank checks, safety deposit box keys and any other items evidencing the obtaining, secreting, transfer, concealment, storage and/or expenditure of money or other assets including, but not limited to, controlled substances;

f. Firearms, ammunition (including spent ammunition), and indicia of firearm possession, including photos and videos depicting firearm possession, gun cases, gun packaging, gun racks, gun manuals, cleaning kits, tools used for the maintenance of firearms, magazines, ammunition, and packaging for magazines or ammunition;

g. Documents and papers evidencing ownership of firearms, possession of firearms, storage and location of such assets and facilities to safely store and secure such items, such as safes, to include lock boxes, gun safes, and strong boxes;

h. Cellular telephones, personal data accessories, computer flash cards, video tapes, compact disks, digital video disks, and other devices and/or electronic media;

i. Photographs, in particular photographs of controlled substances and photographs of individuals possessing controlled substances and photographs showing the association of individuals;

j. Indicia of occupancy, residence, and/or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, and keys;

k. Cryptocurrency seed phrases, cryptocurrency storage media (i.e. cryptocurrency hardware wallets), and cryptocurrency software wallets.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant ("COMPUTER"):

a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. Evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. Evidence of the times the COMPUTER was used;

i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. Records of or information about Internet Protocol addresses used by the COMPUTER;

l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the **TARGET LOCATION**, law enforcement personnel are authorized to press the fingers (including thumbs) and show the faces of individuals found at the **TARGET LOCATION** to the Touch ID or Face ID sensor of cellular phones and/or laptops for the purpose of attempting to unlock the device via Touch ID or Face ID in order to search the contents as authorized by this warrant.